

KSC

IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MARYLAND
Northern Division

FILED _____ ENTERED _____
LOGGED _____ RECEIVED _____

MAY 30 2017

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
DEPUTY

In the Matter of the Search of)
Electronic Account Stored at Premises)
Controlled and Hosted by Facebook,)
Headquartered in Menlo Park,)
California)

Case No. _____

BY
17 - 1387 - ADC

UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Kyra M. Dressler, being duly sworn, hereby state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") currently assigned to the Baltimore Division of the FBI, Joint Terrorism Task Force ("JTTF") and have been so since 2009. As an FBI Agent, my responsibilities have included investigating a variety of criminal offenses, including drug trafficking, violent gang activities, and terrorism-related violations. In the course of my employment with the FBI, I have received extensive training in conducting criminal and counterterrorism investigations and I have authored affidavits in support of search and arrest warrants and testified in Federal trials.

2. On December 11, 2015, Mohamed ELSHINAWY was arrested by agents of the FBI on a criminal complaint charging him with terrorism-related offenses. He was subsequently indicted by a federal grand jury, on January 13, 2016, for providing and attempting to provide material support to ISIL, a foreign terrorist organization, and conspiracy to do the same, in violation of 18 U.S.C. § 2339B; financing of terrorism in violation of 18 U.S.C. § 2339C(a); and making material false statements in violation of 18 U.S.C. § 1001. The charges involve, among other things, ELSHINAWY's receipt of over \$8,000 in funds from ISIL, also known as the Islamic State, for the purpose of committing a terrorist act in the United States.

3. This affidavit is being submitted in support of an application for authorization to

conduct a search of the following electronic account (the “**Target Account**”) stored at premises owned, maintained, controlled, or operated by Facebook, Inc. (“Facebook”), a social networking company headquartered in Menlo Park, California:

Facebook User ID: 100004675178304
User Name: تامر الخضرى
E-mail Address: tamer.elkhodary@yahoo.com

Technical Information Regarding Facebook

4. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, which can then be used to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user’s full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

5. A Facebook user can connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

6. Facebook users may also join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and/or administrator, as well as a PDF of the current status of the group profile page.

7. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

8. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their

Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

9. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

10. Facebook users can exchange private messages on Facebook with other users using an application called Facebook Messenger. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

11. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or

content on third-party (i.e., non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

12. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

13. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace. In addition to all of these applications, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

14. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

15. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

16. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by

the provider or user as a result of the communications.

17. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation. In my training and experience, a Facebook user’s “Neoprint,” IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time.

18. Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner.

19. Finally, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example,

information on the Facebook account may indicate the owner's motive and intent to commit a crime, or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

Probable Cause

20. On June 25, 2015, the FBI became aware of Mohamed Elbarbary, an ISIL facilitator located overseas, who was attempting to send money to the United States, possibly for nefarious purposes. Western Union records confirm that on June 28, 2015, ELSHINAWY received a \$1,000.00 wire transfer emanating from a location in Egypt. Elbarbary was the identified payor and ELSHINAWY was the identified payee with his listed residential address of 335 McCann Street in Edgewood, Maryland. The pay agent was the Short Stop Beverage Barn located at 623 S. Philadelphia Blvd. in Aberdeen, Maryland, near ELSHINAWY's residence.

21. On the same day that ELSHINAWY obtained the wire transfer funds, FBI surveillance agents observed him driving his silver Honda to an M&T Bank Branch located at 1409 Pulaski Highway in Edgewood, where he conducted a transaction at the drive-up ATM. M&T Bank records confirm that ELSHINAWY made a cash deposit at that time into his M&T account in the amount of \$800.00. Video surveillance also provided by M&T Bank further confirmed that ELSHINAWY was the depositor of the \$800.00 cash. Subsequent transactions from M&T Bank reveal that \$200.00 of that deposit was subsequently transferred to another account in the names of ELSHINAWY and his partner, Rachel Rowe.

22. On July 17, 2015, ELSHINAWY consented to a non-custodial interview by Baltimore FBI agents. Upon being questioned about the nature of the \$1,000.00 Western Union transfer, ELSHINAWY claimed that the money had come from his mother who resides in Egypt.

After being shown the Western Union receipt with Elbarbary's name as the sender, ELSHINAWY claimed that the money was to purchase an iPhone for a friend. Upon being advised that making a false statement to law enforcement was a criminal offense for which he could face imprisonment, ELSHINAWY finally revealed that he had a childhood friend by the name of Tamer ELKHODARY who had been previously arrested on terrorism-related offenses in Egypt and had fled to Syria following his release from custody. ELKHODARY subsequently contacted ELSHINAWY on Facebook and they began to communicate on a regular basis. ELSHINAWY admitted that ELKHODARY subsequently introduced him, via social media, to ISIL operatives for the express purpose of receiving funds from ISIL into the United States. Investigators ultimately learned that ELSHINAWY subsequently received a total of at least \$8,700 from individuals/businesses associated with ISIL.

Facebook Accounts/Records

ELSHINAWY Account

23. On July 30, 2015, a search and seizure warrant was issued in the District of Maryland for information contained within ELSHINAWY's Facebook account ID 100001303475553 for the period beginning January 1, 2015, to the date of execution of the warrant. (Case No. 15-1571TJS). Analysis of those records revealed communication with ELKHODARY's Facebook account ID 100004675178304 (i.e., the **Target Account**). Specifically, the two accounts exchanged over 800 messages from February 16 through July 25, 2015. However, the overwhelming majority of those messages had been deleted from ELSHINAWY's account.

ELKHODARY Accounts

24. On October 19, 2015, and February 16 and September 9, 2016, search and seizure warrants were issued in the District of Maryland for information contained within two of ELKHODARY's Facebook accounts. Specifically, data was received from the **Target Account** (Case Nos. 15-2245SAG and 16-0503JMC) for the period from January 1, 2015 through February 16, 2016, and from ID 100009842760994 (Case No. 16-2382SAG) for the period from May 1 through June 30, 2015

25. The search warrant results on the **Target Account** revealed chats between ELKHODARY and other ISIL associates regarding operational planning to support ISIL operatives overseas. For example, one of those chats included ELKHODARY's self-admission that he was a member of ISIL.

26. The **Target Account** results also revealed the substance of numerous chats between ELSHINAWY and ELKHODARY related to their association with, and activities on behalf of, ISIL, including discussions regarding ELSHINAWY's allegiance to ISIL and ELKHODARY's advice to ELSHINAWY regarding activities in support of ISIL's cause. For example, during a chat on February 17, 2015, ELSHINAWY pledged his allegiance to ISIL, described himself as its soldier, asked ELKHODARY to convey his message of loyalty to ISIL leadership, and committed himself to committing violent jihad. ELKHODARY cautioned ELSHINAWY not to discuss his plans for a potential terrorist attack with anyone, to which ELSHINAWY agreed, acknowledging that committing such an attack would be a crime in the United States.

27. Notably, the seized records from the **Target Account** reveal no ISIL-related conversations between ELKHODARY and ELSHINAWY prior to the chat in which

ELSHINAWY pledged his allegiance on February 17, 2015.¹ Based on the content of this communication – including the specific pledge and instructions – your Affiant submits that it is unlikely that this is the first ever Facebook communication that the two would have had about ISIL and ISIL-related topics. Rather, it is likely that the two would have had communications about these topics prior to January 1, 2015 (i.e., the date of the earliest records previously sought from this account). Moreover, your Affiant submits that there is probable cause to believe that ELKHODARY – who had Facebook discussions about ISIL operations and operatives – would likely have also had earlier Facebook conversations with ISIL associates other than ELSHINAWY. Thus, the request search warrant for 2014 records on the **Target Account** is likely to reveal important evidence related to this investigation.

28. A review of IP logs obtained for ELSHINAWY's Facebook account 100001303475553 indicated that ELSHINAWY was using his Facebook account as early as January 3, 2015. Recently-obtained Facebook business records indicate that the **Target Account** was active during 2014. Specifically, internet login records reveal that the account was accessed approximately 75 times between April 26, 2014 and December 11, 2014.

29. ELSHIANWY received his first ISIL-sponsored payment on or about March 23, 2015. ELSHINAWY never revealed his receipt of this payment, or a number of others that followed, during the course of his non-custodial interviews with FBI agents in July 2015. Given the nature of the conversation with ELKHODARY on February 17, 2015, and the fact that ISIL-

¹ As noted above, investigators also received records for ELKHODARY's Facebook account 100009842760994. The results from this account, however, were more limited in scope, covering only the period from May 1 through June 30, 2015. Moreover, the seized records from this account revealed no apparent ISIL-related conversations with ELSHINAWY. As a result, your Affiant believes it likely that communications about ISIL-related topics with ELSHINAWY and others would have taken place over the **Target Account**.

related funds made their way to ELSHINAWY not long thereafter, it is more likely that substantive discussions regarding ELSHINAWY's mindset regarding ISIL, and his willingness to receive monies from ISIL to support a terrorist attack were discussed in more detail prior to ELSHINAWY's pledge of allegiance to the organization on February 17, 2015.

30. ELKHODARY is referenced as an unnamed coconspirator in the pending indictment against ELSHINAWY and the investigation into ELKHODARY's role continues. It is your affiant's belief that there is probable cause to believe that within ELKHODARY's Facebook account 100004675178304 there exists evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2339B and 2339C. This evidence likely consists of additional ISIL-related communications between ELKHODARY and others, including ELSHINAWY, similar to those communications previously obtained through execution of the search warrants referenced above, including communication regarding the transfer of monies to ELSHINAWY from ISIL members, operational planning regarding use of the monies, and the mindset of the identified subjects regarding ISIL and related activities. For these reasons, your affiant requests authorization for a warrant to conduct a search of information contained within ELKHODARY's Facebook account identified in paragraph 3 above, for the period from January 1 through December 31, 2014.

Conclusion

31. This warrant application is governed by 18 U.S.C. § 2703(a), which permits governmental entities to require disclosure of the contents of stored electronic communications pursuant to a search warrant. Section 2703(a) further provides that such a warrant may be issued by a court with jurisdiction over the offense under investigation. Pursuant to § 2703(b)(1)(A), notice to the subscriber of such a disclosure pursuant to a warrant is not required. In addition, §§

2703(c)(1)(A) and (c)(2) provide that, in addition to the contents of electronic communications, the government may obtain by means of a search warrant any remaining types of records and information, such as computer logs and subscriber information, pertaining to a subscriber of an electronic communication service or remote computing service. Section 2703(c)(3) provides further that under such circumstances, no notice to the subscriber or customer is required.

32. Your affiant also requests that the Court issue an order, pursuant to 18 U.S.C. § 2705(b), commanding Facebook not to notify any person, including the account subscribers, of the existence of the warrant until further order of the Court, as there is reason to believe that notification of the existence of the warrant will result in possible destruction of, or tampering with, evidence, which would seriously jeopardize the ongoing investigation. In addition, notification of the warrant and nature of the ongoing investigation, now or in the future, may result in targets of the investigation changing their patterns of behavior, especially with regard to the accounts in question, and thereby potentially conceal further activities related to conduct that is the subject of the investigation. Your affiant knows from his criminal experience and training that subjects of criminal investigations will often destroy digital evidence, or stop utilizing electronic accounts, upon learning of the existence of an investigation involving them and/or their associates. Additionally, if Facebook notifies anyone that a warrant has been issued to the subject accounts, the targets of this investigation and other persons may seek to further mask their identities and criminal conduct, thereby seriously jeopardizing the ongoing investigation.


33. In order to ensure that agents search only those computer accounts and/or files described in Attachment A, this affidavit and application for a search warrant seeks authorization to permit employees of Facebook to assist agents in the execution of this warrant. To further

ensure that agents executing this warrant search only those items described in Attachment A, the following procedures will be implemented:

a. The agent executing the warrant shall effect service by any lawful method, including uploading the warrant to Facebook's law enforcement web portal. Facebook personnel will be directed to isolate the items described in Attachment A and create an exact duplicate, in electronic form, of the items identified in Attachment A to provide to the agent who serves this warrant.

b. Upon receipt of this information, the search procedures outlined in Attachment B will be utilized to minimize, to the greatest extent possible, the likelihood that files or other information for which there is not probable cause to search are viewed.

Your affiant has signed this document under oath as to all assertions and allegations contained herein. Your affiant also states that the representations herein are true and correct to the best of his knowledge of the underlying investigation, and reliable information provided by other law enforcement personnel involved in this matter.


Kyra M. Dressler, Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 11th day of May, 2017.


A. David Copper
United States Magistrate Judge

KSC

ATTACHMENT A

I. Facebook Account to be Searched

Facebook User ID: 100004675178304

II. Information to be disclosed by Facebook

To the extent that the information described herein is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the account identified above for the period from January 1, 2014 to December 31, 2014 for Facebook ID 100004675178304:

- a. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities, including dates of deletion of friends, accounts, or communications.
- c. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them.
- d. All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings;

rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

e. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending “Friend” requests.

f. All “check ins” and other location information.

g. All IP logs, including all records of the IP addresses that logged into the account.

h. All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked.”

i. All information about the Facebook pages of which the account is or was a “fan.”

j. All past and present lists of friends created by the account.

k. All records of Facebook searches performed by the account.

l. All information about the user’s access and use of Facebook Marketplace.

m. The types of service utilized by the user.

n. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number).

o. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account.

p. All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken.

III. Information to be seized by the government

All information described above in Section II, including supporting images and visual depictions, pertaining to the following matters and that constitutes fruits, evidence and instrumentalities of the following offenses: providing and attempting to provide material support to a foreign terrorist organization, and conspiracy to do same, in violation of 18 U.S.C. § 2339B; the unlawful financing of terrorism in violation of 18 U.S.C. § 2339C; and making material false statements in violation of 18 U.S.C. § 1001. The records to be searched are for the period from January 1, 2014 to December 31, 2014 for Facebook ID 100004675178304:

- a. Records of communication with other individuals concerning the preparation for, planning of, and/or funding of terrorist-related activities.
- b. Information pertaining to the solicitation and/or identification of co-conspirators and/or facilitators involved or associated with Mohammed ELSHINAWY, Tamer ELKHODARY, Ahmed Elshinawy, a/k/a Abo Alkhair, and others involved in undertaking terrorist-related activity in the United States or elsewhere.
- c. Information pertaining to monetary transfers, financial accounts or other monetary instruments connected to terrorist-related planning or attacks.
- d. Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime.
- e. All records relating to who created, used, or communicated with the User ID, including records about their identities and whereabouts, screen names, and payment methods.

f. Account history (including Terms of Service and any complaints) and billing records (including date, time, duration, and screen names used each time the account was activated).

g. A complete log file of all activity relating to the account (including dates, times, method of connection, port, dial-up, dedicated phone numbers, and/or locations).

ATTACHMENT B

Description of Methods to be Used for Searching Electronically Stored Information

This warrant authorizes the search of electronically stored information. The search shall be conducted pursuant to the following protocol in order to minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search are viewed.

With respect to the search of any digitally/electronically stored information seized pursuant to the instant warrant as described in Attachment A hereto, the search procedure may include the following techniques (the following is a non-exhaustive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized;
- c. physical examination of the storage device, including surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized;
- d. opening or reading portions of files in order to determine whether their contents fall within the items to be seized;
- e. scanning storage areas to discover data falling within the list of items to be seized, to possibly recover any such deleted data, and to search for and recover files falling within the list of items to be seized; and/or
- f. performing key word searches through all electronic storage areas to determine whether occurrence of language contained in such storage areas exist that are likely to appear in the evidence to be seized.